UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/752,420 | 01/05/2004 | Gregory Gordon Rose | 030010 | 3858 |

23696 7590 08/03/2011

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

| EXAMINER | |
|---|---|
| ZECHER, CORDELIA P K | |
| ART UNIT | PAPER NUMBER |
| 2432 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 08/03/2011 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/752,420 | ROSE ET AL. | |
| | Examiner | Art Unit | |
| | CORDELIA ZECHER | 2432 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *22 June 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3,5-24,26-28,50,51 and 53-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-24,26-28,50,51 and 53-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments filed June 22, 2011 have been fully considered but they are not persuasive.

2. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

3. Applicant argues that modifying Arthan to include the central system as part of the source system would be completely arbitrary and require an unsupported redesign of the architecture depicted in Arthan. More specifically, applicant argues that in the only figure in Arthan the central system and the source system are shown as two separate devices and therefore never intended to be part of a single system. However, as explained in the previous office action, it is the examiner's position that Arthan suggests to an ordinarily skilled artisan modifying the central system and the source system into a single system because Arthan states that the source system may be a complex distributed system and may comprise a large number of physically separate nodes

(column 2, lines 30-34). Therefore, the central system could be one of the nodes of the distributed source system.

4. Applicant argues that characterizing the central system as being integrated into the source system renders some of Arthan obsolete. More specifically, applicant argues that the private key is distributed in a secure manner using the KEK, and that it would be unnecessary and superfluous to transmit the private key to the source system if they are part of the same system. However, in the embodiment that the source system is a complex distributed system comprising a large number of nodes (column 2, lines 30-34), the source system would be required to send data between the separate nodes, potentially including the private key. Therefore the distributed embodiment of the source system would require sending data between the nodes, and would not be unnecessary or superfluous.

5. Applicant argues that Arthan teaches away from integrating the central system with the source system. "What the prior art teaches and whether it teaches toward or away from the claimed invention ... is a determination of fact." *Para-Ordnance Mfg., Inc. v. SGS Importers Int'l, Inc.*, 73 F.3d 1085, 1088 (Fed. Cir. 1995). "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994).

6. More specifically, applicant argues that Arthan teaches that the operators of the source system are not authorized to handle the private key itself, and that a security

officer controls the central system, and the keys. However, Arthan's reference to the operators of the source system not being authorized to handle the private key itself is merely an example (column 2, lines 35-38), and therefore not a requirement. Therefore the security office that handles the changes to the keys (column 5, lines 7-10), could be an operator of the source system.

7. Applicant has not pointed to an explicit disclosure within Arthan that acts to "criticize, discredit, or otherwise discourage" integrating the central and source system. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). Therefore, applicant has not shown that Arthan's disclosure teaches away.

8. Applicant argues that the central system output's the first private key, which is the opposite of the claimed invention which teaches storing the first private key and outputting the second private key. In addition, applicant argues that the central system does not use any of the keys for authentication. For the purposes of clarification, the examiner will explain how each system in Arthan is being cited to teach each limitation. The central system is cited for generating the first and second private and public key pairs (column 4, lines 25-30). The source system is cited for storing the first private key (column 2, lines 48-50) and using the first private key (column 4, lines 15-23) for authentication (column 1, lines 37-40). Arthan does not explicitly disclose that the second private key is actually transmitted, Kurn teaches that the protection key is divided into shares and shared with the owners (paragraph 89), and once the shares are sent that the key is erased from memory (paragraph 102). Therefore the combination of the central/source system configuration of Arthan in view of Kurn

teaches a generating a first and second private key, storing a first private key which is used for authentication and outputting the second private key such that it is not stored in the storage medium.

9. Applicant argues that integrating the central system and source system of Arthan would show insight that is contrary to the understanding and expectations of the art. More specifically, applicant argues that Arthan expresses the requirement that the operators of the source system are not authorized to handle the private key itself. However, as explained above, the cited portion of Arthan is merely an example, and not an express requirement. Therefore the security office that handles the changes to the keys (column 5, lines 7-10), could be an operator of the source system.

10. It is noted that simply stating that the references fail to teach or suggest the entire claim, while bolding certain limitations, is not a separate patentability argument. Therefore, applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

11. Applicant argues that each of the independent claims, and the corresponding dependent claims, are allowable for reasons similar to those discussed above. However, as explained above, the arguments are not persuasive.

***Information Disclosure Statement***

12. The information disclosure statement (IDS) submitted on June 23rd, 2011 was filed after the mailing date of the Non-Final Rejection on March 24th, 2011. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

***Claim Rejections - 35 USC § 103***

13. Claims 50, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan et al's US Patent 6,782,103 B1, and in view of Kurn et al's US Publication 2002/0071561 A1.

14. Referring to claim 50, Arthan teaches:

a. A processor configured to generate a first private key and corresponding first public key, generate a second private key associated with the first private key and to create a second public key corresponding to the second private key (column 4, lines 25-30).

b. A storage medium coupled to the processor to store the first private key (column 2, lines 48-50).

c. A second private key that can be used when there is no access to the first private key wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 25-32).

d. Output the first public key and the second public key to a verifier device (column 4, lines 18-20).

e. Wherein the processor uses the stored first private key for authentication of the device prior to using the second private key (column 4, lines 15-23).

15. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

16. Referring to claim 56, Arthan teaches the second private key is removed from the user device upon transmission of the second private key (column 4, lines 30-32).

17. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to

include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

18. Claims 1 – 3, 5 – 9, 11 – 14, 16 – 24, 26 – 28, 51, 53 – 55, and 57 – 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan et al's US Patent 6,782,103 B1, and in view of Kurn et al's US Publication 2002/0071561 A1 and further in view of Hansmann et al's US Publication 2002/0018570 A1.

19. Referring to claims 1, 14 and 22, Arthan teaches:

f. Creating a first private key and corresponding public key (column 4, lines 25-30).

g. Creating a second private key associated with the first private key and creating a second public key corresponding to the second private key (column 4, lines 25-30).

h. The second private key being used when the first private key is inaccessible (column 4, lines 25-32).

i. Transmitting the first public key and the second public key to a verifier device (column 4, lines 18-20).

j. Using the first private key for authentication prior to using the second private key (column 4, lines 15-23).

20. Arthan fails to teach outputting the private key such that it is not stored on the user device by transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Kurn teaches that the

protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

21. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

22. Referring to claims 2 and 23, Kurn teaches:

k. Creating at least two shares of the private key at the device (paragraph 89).

l. Outputting each share to a different entity (paragraph 89).

23. Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to

modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

24. Referring to claims 3, 16, and 24, Arthan teaches using the second private key independent of the first private key for authentication (column 4, lines 20-23). Kurn teaches re-creating the private key using at least some shares of the plurality of shares (paragraphs 27 and 103). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

25. Referring to claims 5 and 17, Arthan teaches:

m. Creating a third private key associated with the second private key, and creating a third public key corresponding to the third private key (column 5, lines 12-14).

n. Outputting the third public key to the verifier (column 5, lines 12-14).

26. Referring to claim 6, Arthan teaches:

o. Outputting the third private key (column 4, lines 30-32).

p. Using the third private key for authentication (column 4, lines 20-23).

27. Kurn teaches:

q. Outputting the key as a plurality of shares such that it can be recreated (paragraph 89).

r. Recreating the private key using at least some of the plurality of shares (paragraph 27).

28. Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

29. Referring to claim 7, Arthan teaches that the second private and public keys are created independently from the first private and public keys (column 4, lines 25-26).

30. Referring to claims 8 and 18, Arthan teaches:

s. Creating a third private key associated with the second key and creating a third public key corresponding to the third private key (column 5, lines 12-14).

t. Creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key (column 4, lines 25-30).

u. Outputting the third and fourth public keys (column 4, lines 18-20).

31. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89). Arthan and Kurn

are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

32. Referring to claim 9, Arthan teaches:

v. Disabling use of the second private key for authentication (column 4, lines 20-23).

w. Using the third private key for authentication (column 4, lines 20-23).

x. Accessing the fourth private key (column 4, lines 20-23).

y. Using the fourth private key for authentication (column 4, lines 20-23).

33. Arthan fails to teach recreating the fourth private key. However, Kurn teaches using the shares to recreate the key (paragraph 27). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

34. Referring to claims 11, 19, and 26, Arthan discloses:

z. Receiving a first public key, wherein the first public key has a corresponding first private key stored in the user device (column 4, lines 18-23).

aa. Receiving a second public key, the second public key associated with the first public key (column 4, lines 18-20), wherein the second public key has a corresponding second private key that can be used when there is no access to a first private key corresponding to the first public key wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 25-32).

bb. Using the first public key for authentication (column 5, lines 12-14).

cc. Using the second public key for authentication if the first public key fails (column 5, lines 12-14).

35. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

36. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the

same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

37. Referring to claims 12, 20 and 27, Arthan teaches receiving a third public key from the device, the third public key associated with the second public key (column 5, lines 12-14), if the first public key fails and the second key results in successful authentication (column 4, lines 20-23).

38. Referring to claims 13, 21, and 28, Arthan teaches a third public key and a fourth public key from the device (column 5, lines 12-14), if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second key (column 4, lines 20-26).

39. Referring to claim 51, Arthan teaches:

dd. A receiver configured to receive a first public key from a device and receiving a second public key from the device, wherein the first public key has a corresponding first private key stored on the user device and the second public key associated with the first public key, wherein the second public key has a corresponding second private key that can be used when there is no access to a first private key corresponding to a first public key, wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 15-30).

ee. A storage medium coupled to the receiver configured to store the first and second public keys (column 4, lines 18-20).

ff. A processor coupled to the receiver and the storage medium, the processor configured to use the first public key for authentication, the processor configured to use the second public key for authentication if the first public key fails (column 4, lines 18-20).

40. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

41. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to

include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

42. Referring to claims 53 – 55, Arthan teaches the second private key is removed from the user device upon transmission of the second private key (column 4, lines 30-32).

43. Arthan fails to teach transmitting a plurality of shares of the private key to a plurality of different entities such that it can be recreated while the private key is not stored on the device. However, Kurn teaches that the protection key is split among multiple individuals (paragraph 89) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

44. Referring to claims 57, 61 and 65, Arthan teaches:

gg. Retrieving a second private key at a mobile user device that has no access to a first private key associated with the second private key (column 5, lines 12-14).

hh. Creating a third private key and a corresponding third public key (column 5, lines 12-14).

ii. Using the second private key for authentication before using the third private key (column 4, lines 20-23).

45. Arthan fails to teach recreating a key using at least some shares of a plurality of shares of the private key, or outputting the private key such that it is not stored on the user device. However, Kurn teaches that the protection key is split among multiple individuals, wherein the protection key can be recreated using seven shares of the private key (paragraphs 89-90) and that after the key is encoded, the protection key is erased from the computer memory (paragraph 102). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

46. Arthan in view of Kurn fails to teach a mobile user device. However, Hansmann teaches authenticating devices, the devices including mobile phones (paragraphs 27-28). Arthan in view of Kurn and Hansmann are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan in view of Kurn and Hansmann before him or her, to modify the system of Arthan in view of Kurn to include the mobile phone of Hansmann. The suggestion/motivation for doing so would have been mobile phones are well known devices used for communication.

47. Referring to claim 58, 62 and 66, Kurn teaches recreating the second private key at a user device different from a user device that created the first private key and second private key (paragraph 94). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

48. Referring to claims 59, 63, and 67, Arthan teaches:

jj. Outputting the third private key while retaining the second private key (column 4, lines 30-32).

kk. Transmitting the third public key to the verifier device (column 4, lines 18-20).

49. Kurn teaches outputting the key as a plurality of shares such that it can be recreated (paragraphs 89-90). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

50. Referring to claims 60, 64, and 68, Arthan teaches:

ll. Creating a fourth private key and a corresponding fourth public key (column 4, lines 25-30).

mm. Outputting the fourth private key while retaining the third private key (4, lines 30-32).

nn. Outputting the third and fourth public keys (column 4, lines 18-20).

51. Kurn teaches outputting the key as a plurality of shares such that it can be recreated (paragraphs 89-90). Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

52. Claims 10 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan in view of Kurn in view of Hansmann as applied above, and further in view of Official Notice. Referring to claim 10, Arthan in view of Kurn in view of Hansmann discloses all the limitations of the parent claim. Arthan in view of Kurn in view of Hansmann does not explicitly disclose preventing retransmission of the second private key. However, Arthan teaches that the key is encrypted and stored securely (column 5, lines 26-28) and that it should be held securely after generation (column 4, lines 30-31). The examiner takes official notice that it would have been obvious, to one of ordinary skill in the art at the time of invention, to prevent retransmission of the key since keeping

the key stored securely is important and that retransmission would expose the key to more vulnerabilities.

53. Referring to claim 15, Kurn teaches:

oo. Creating at least two shares of the second private key at the device (paragraph 89).

pp. Outputting each share to a different entity (paragraph 89).

54. Arthan and Kurn are analogous art because they are from the same field of endeavor, cryptography. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Kurn before him or her, to modify the system of Arthan to include the key split of Kurn. The suggestion/motivation for doing so would have been so that no one individual can produce the key (paragraph 27).

55. Arthan in view of Kurn does not explicitly disclose subsequent outputting of the key is prevented. However, Arthan teaches that the key is encrypted and stored securely (column 5, lines 26-28) and that it should be held securely after generation (column 4, lines 30-31). The examiner takes official notice that it would have been obvious, to one of ordinary skill in the art at the time of invention, to prevent retransmission of the key since keeping the key stored securely is important and that retransmission would expose the key to more vulnerabilities.

***Conclusion***

56. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA ZECHER whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CORDELIA ZECHER/
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432